PATENT
81940.0054
Express Mail Label No. EV 325 216 828 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Art Unit: Not assigned
Hiromi UKAI et al.	Examiner: Not assigned
Serial No: Not assigned	
Filed: July 15, 2003	
For: METHOD AND APPARATUS FOR USING CONTENTS	

TRANSMITTAL OF PRIORITY DOCUMENT

Mail Stop PATENT APPLICATION
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2002-321962 which was filed November 6, 2002, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: July 15, 2003

By: _____
Anthony J. Orler
Registration No. 41,232
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年１１月　６日

出願番号
Application Number:　特願２００２－３２１９６２

[ST.10/C]:　[ＪＰ２００２－３２１９６２]

出願人
Applicant(s):　株式会社日立製作所

２００３年　４月１１日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０２５１９１

【書類名】　特許願

【整理番号】　K02006801A

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/60

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　鵜飼　ひろみ

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　平澤　茂樹

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　安細　康介

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　越前　功

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　吉浦　裕

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　岡山　祐孝

【発明者】

【住所又は居所】　東京都千代田区神田駿河台四丁目６番地　株式会社日立製作所デジタルメディアグループ内

【氏名】　田胡　修一

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ保護システム

【特許請求の範囲】

【請求項１】

プロバイダを識別するための第１のプロバイダＩＤがコンテンツ保証機関によって埋め込まれたデジタルコンテンツを保持すると共にプロバイダを識別するための第２のプロバイダＩＤが認証局によって埋め込まれた証明書を保持するプロバイダ装置から、前記デジタルコンテンツの提供を受けるコンテンツ利用端末において、

前記デジタルコンテンツと前記証明書を、前記プロバイダ装置から受信する受信処理部と、

前記証明書を用いて前記プロバイダが前記認証局によって許可されているか否かをチェックする第１のチェック処理部と、

前記証明書から前記第２のプロバイダＩＤを読み出し、読み出された前記第２のプロバイダＩＤと受信された前記デジタルコンテンツとを互いに対応付けて記録媒体へ記録する記録処理部と、

前記デジタルコンテンツから前記第１のプロバイダＩＤを検出する検出処理部と、

前記記憶媒体から前記第１のプロバイダＩＤを読み出し、前記第１のプロバイダＩＤと前記第２のプロバイダＩＤとを比較し、両プロバイダＩＤが一致するか否かを判断する第２のチェック処理部と、

前記デジタルコンテンツを利用する利用処理部を備えたコンテンツ利用端末。

【請求項２】

請求項１に記載のコンテンツ利用端末において、

前記利用処理部は、前記チェック処理部が前記両プロバイダＩＤが一致しないと判断した場合に、前記デジタルコンテンツの利用を制限するコンテンツ利用端末。

【請求項３】

請求項１に記載のコンテンツ利用端末において、

前記第１のプロバイダＩＤは、前記コンテンツ保証機関によって、電子透かしにより前記デジタルコンテンツに埋め込まれているコンテンツ利用端末。

【請求項４】

請求項１に記載のコンテンツ利用端末において、

前記両プロバイダＩＤが一致しないと判断した場合に、前記認証局と前記コンテンツ保証機関と前記コンテンツ・ホルダーの少なくとも１つへ通知する通知処理部を備えたコンテンツ利用端末。

【請求項５】

請求項４に記載のコンテンツ利用端末において、

前記通利処理部は、前記両プロバイダＩＤが一致しないと判断した場合に、前記認証局と前記コンテンツ保証機関と前記コンテンツ・ホルダーの少なくとも１つへ、前記第１のプロバイダＩＤと前記第２のプロバイダＩＤの少なくとも１つを通知するコンテンツ利用端末。

【請求項６】

請求項１に記載のコンテンツ利用端末において、

前記検出処理部は、前記デジタルコンテンツから前記第１のプロバイダＩＤを検出できない場合に、前記デジタルコンテンツの流通経路が管理対象外であると判断し、

前記チェック処理部は、前記両プロバイダＩＤが一致しないと判断した場合に、前記デジタルコンテンツの流通経路が不正であると判断するコンテンツ利用端末。

【請求項７】

請求項１に記載のコンテンツ利用端末において、

前記記録媒体は、前記デジタルコンテンツを格納するためのコンテンツ蓄積部と、前記コンテンツ蓄積部に比較して耐タンパ性が高くかつ前記第２のプロバイダＩＤを格納するためのライセンス管理部とを有するコンテンツ利用端末。

【請求項８】

請求項１に記載のコンテンツ利用端末において、

前記デジタルコンテンツは、前記コンテンツ・ホルダを識別するためのコンテ

ンツＩＤを、前記コンテンツ保証機関又は前記コンテンツ・ホルダによって埋め込まれ、

前記検出処理部は、前記デジタルコンテンツから前記第１のプロバイダＩＤを検出できない場合に、前記デジタルコンテンツの流通経路が管理対象外であると判断し、さらに、前記デジタルコンテンツの流通経路が管理対象外であると判断した場合に、受信された前記デジタルコンテンツから前記コンテンツＩＤを検出し、

前記利用処理部は、前記デジタルコンテンツに前記コンテンツＩＤが埋め込まれていないと判断した場合に、前記デジタルコンテンツの利用を許可するコンテンツ利用端末。

【請求項９】

請求項１に記載のコンテンツ利用端末において、

前記デジタルコンテンツは、当該コンテンツ利用端末を識別するための第１のユーザＩＤを、前記プロバイダ装置によって埋め込まれ、

前記記録媒体は、当該コンテンツ利用端末を識別するための第２のユーザＩＤを記憶し、

前記検出処理部は、前記第２のチェック処理部が前記両プロバイダＩＤが一致すると判断した場合に、前記デジタルコンテンツから前記第１のユーザＩＤを検出する検出し、

前記第２のチェック処理部は、前記記憶媒体から前記第２のユーザＩＤを読み出し、前記第１のユーザＩＤと前記第２のユーザＩＤとを比較し、両ユーザＩＤが一致するか否かを判断するコンテンツ利用端末。

【請求項１０】

デジタルコンテンツを端末へ提供するプロバイダ装置において、

プロバイダを識別するための第１のプロバイダＩＤがコンテンツ保証機関によって埋め込まれたデジタルコンテンツを記憶すると共にプロバイダを識別するための第２のプロバイダＩＤが認証局によって埋め込まれた証明書を記憶する記憶装置と、

前記端末からの要求に応答して、前記証明書を前記端末へ送信する第１の送信

処理部と、

前記端末が前記証明書を用いて前記プロバイダが前記認証局によって許可されているか否かをチェックすると共に前記証明書から前記第２のプロバイダＩＤを読み出し、読み出された前記第２のプロバイダＩＤと受信された前記デジタルコンテンツとを互いに対応付けて記録媒体へ記録した場合に、前記端末からの要求に応答して、前記デジタルコンテンツを前記端末へ送信する第２の送信処理部とを備え、

前記端末は、受信された前記デジタルコンテンツから前記第１のプロバイダＩＤを検出し、前記記憶媒体から前記第１のプロバイダＩＤを読み出し、前記第１のプロバイダＩＤと前記第２のプロバイダＩＤとを比較し、両プロバイダＩＤが一致するか否かを判断するプロバイダ装置。

【請求項１１】

当該コンテンツ利用端末を識別するための第１のユーザＩＤをデジタルコンテンツに埋め込むプロバイダ装置から、前記デジタルコンテンツの提供を受けるコンテンツ利用端末において、

当該コンテンツ利用端末を識別するための第２のユーザＩＤを記憶する記憶装置と、

前記デジタルコンテンツを、前記プロバイダ装置から受信する受信処理部と、

受信された前記デジタルコンテンツを前記記録装置へ記録する記録処理部と、

前記デジタルコンテンツから前記第１のユーザＩＤを検出する検出処理部と、

前記記憶部から前記第２のユーザＩＤを読み出し、前記第１のユーザＩＤと前記第２のユーザＩＤとを比較し、両プロバイダＩＤが一致するか否かを判断するチェック処理部とを備えたコンテンツ利用端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタルコンテンツの流通経路を管理するためのシステム及び方法に関する。

【０００２】

【従来の技術】

【特許文献１】特開2000-330873号公報

【特許文献２】特開2001-256192号公報

近年、ストリーミング技術やデータ圧縮技術が進歩すると共に、ブロードバンド通信が急速に家庭に普及し始めたことから、動画や音楽などの大容量のデジタルコンテンツが流通し始めている。デジタルコンテンツはコピーや加工が容易にでき、しかも、品質劣化が生じないという利点がある一方で、不正な利用によって著作権が侵害されるという問題も大きい。

【０００３】

この問題に対して、デジタルコンテンツを暗号化して鍵をかけ、その鍵を別途ライセンスとして利用者／利用端末に配布することで著作権を保護する方式がある。コンテンツの利用時には、システムがライセンスの有無やライセンスに含まれている利用条件情報を参照し、利用期限などの利用条件を満たしている場合のみ、コンテンツが利用できる仕組みになっている。この方式によれば、コンテンツが不正にコピーされても、ライセンスを持たない利用者はコンテンツを利用することはできない。更に、鍵の生成過程に端末固有の番号を組み込むなどして利用端末毎に異なる鍵を生成して配布し、コンテンツと共にライセンスを他の端末にコピーしても、コピー先の端末では鍵が利用できないようにすることによって、コンテンツの不正利用を防ぐ方式もある。

【０００４】

また、電子透かし（Digital watermark）を用いてデジタルコンテンツに著作権情報を埋めこみ、不正利用を検出する技術も提案されている。例えば、特許文献１には、ウェブページなどで利用されるコンテンツに電子透かしで識別情報を埋めこんでおき、利用許可ＤＢに識別情報と利用条件を登録しておき、監視センターがコンテンツに埋めこまれた識別情報と利用許可ＤＢの識別情報とを照合して不正利用を検出する技術が開示されている。また、特許文献２には、購入対象コンテンツを特定する情報とコンテンツ配信者と購入者ごとに割り振られたＩＤ番号を、透かし情報として、流通するコンテンツデータに埋め込むことが開示されている。

【０００５】

【発明が解決しようとする課題】

上記のライセンスを用いた従来技術では、ライセンス情報が改ざんされたり、暗号が解かれたコンテンツが不正に流通する可能性があった。また、コンテンツが流出した場合は、どこから流出したのかを特定する手段がなく、流出を止めることが難しかった。

【０００６】

上記の電子透かしを用いて不正利用を監視する従来技術では、ウェブページへの不正な掲載を監視することは可能であるが、ユーザ端末間でコンテンツをコピーするなど、監視センターからアクセスできない場所での不正利用を監視することはできなかった。また、現在、ウェブページ上では膨大な数のコンテンツが利用されているが、その全てを監視することは困難である。

【０００７】

本発明の目的は、コンテンツ・ホルダとコンテンツ利用者の片方又は双方に対しデジタルコンテンツの流通経路を保証するシステム及び方法を提供することである。

【０００８】

本発明の目的は、デジタルコンテンツの不正流通を抑制するシステム及び方法を提供することを提供することである。

【０００９】

【課題を解決するための手段】

本発明は、コンテンツおよびコンテンツのプロバイダの身元を保証するための認証局を設け、認証局からコンテンツを配信する許可を受けたプロバイダにのみ、認証局が証明書を発行する。証明書にはプロバイダを一意に識別するための識別子（プロバイダＩＤ）が記されている。プロバイダＩＤは認証局が管理して発行する。コンテンツ・ホルダは認証局によって身元が保証されているプロバイダ、すなわち、認証局発行の証明書を所有するプロバイダにコンテンツの配信を依頼する。プロバイダを許可制にすることにより、コンテンツの流通経路を特定することが可能となる。

【００１０】

コンテンツ･ホルダからコンテンツプロバイダへのコンテンツの仲介は、認証局が認定したコンテンツ保証機関が行なう。コンテンツ保証機関は、コンテンツをコンテンツ・ホルダから受け取り、プロバイダのプロバイダＩＤを電子透かしを用いて埋めこみ、埋めこんだＩＤに対応するコンテンツプロバイダに渡す。一度書きこまれたプロバイダＩＤは書き換えできないようにする。これにより、プロバイダが流通経路を改ざんできなくなる。

【００１１】

プロバイダはコンテンツを端末に配信するが、そのコンテンツはコンテンツ保証機関を仲介してコンテンツ・ホルダから受け取ったコンテンツであり、自分自身を示すプロバイダＩＤが透かしで挿入されている。また、プロバイダは認証局から発行された証明書を所有しており、その証明書には自分自身を示すプロバイダＩＤが記載されている。

【００１２】

利用者端末では、プロバイダが所有する証明書を参照し、プロバイダが認証局によって保証されていることを確認してからコンテンツを受信する。受信したコンテンツはコンテンツ蓄積部に記憶されるが、このとき、コンテンツを端末内で一意に識別するためのコンテンツ名とプロバイダを識別するためのプロバイダＩＤとを耐タンパ領域に記憶する。耐タンパ領域とは、外部からの不正なアクセスに備えるための物理的・論理的構造を備えた領域である。端末には透かし検出機能を設け、コンテンツの利用時には、コンテンツ保証機関によってコンテンツに埋め込まれたプロバイダＩＤの透かしを検出し、利用者による書き換えが不能な領域に記憶されたプロバイダのプロバイダＩＤと透かしのプロバイダＩＤとが一致しているかどうかを確認する。一致している場合には、コンテンツの流通経路は正規であると判断してコンテンツを利用できるようにし、一致しない場合にはコンテンツの流通経路は不正であると判断してコンテンツの利用を中断してコンテンツ保証機関に通知する。これにより、不正な経路で流通しているコンテンツとそのプロバイダを検出できるようになる。また、ネットポリスを設けることなく、端末で不正が検出できるようになる。

【００１３】

【発明の実施の形態】

図１は、本発明の一実施例の全体の構成を示した図である。本発明の実施の形態のコンテンツ保護システムは、デジタルコンテンツ（以下、単に「コンテンツ」という）およびプロバイダ４０の身元を保証する認証局１０と、コンテンツ（又はコンテンツの著作権等）を所有するコンテンツ・ホルダ２０と、コンテンツを仲介するコンテンツ保証機関３０と、コンテンツを利用者の端末５０へ提供（配信）するプロバイダ４０と、利用者がコンテンツを利用するための端末５０とを有する。コンテンツ保証機関３０とプロバイダ４０は、認証局１０の許可が必要である。認証局１０とプロバイダ４０の間、認証局１０とコンテンツ保証機関３０の間、コンテンツ・ホルダ２０とコンテンツ認証機関３０の間、コンテンツ保証機関３０とプロバイダ４０の間、プロバイダ４０と端末５０の間は夫々、ネットワークを介して接続可能であるのが好ましい。但し、認証局１０とプロバイダ４０の間、認証局１０とコンテンツ保証機関３０の間は、ネットワークを介して接続されなくてもよい。任所局１０、コンテンツ・ホルダ２０、コンテンツ保証機関３０、プロバイダ４０、端末５０は夫々、処理装置（ＣＰＵ）、記憶装置、通信装置を備えるのが好ましい。さらに、端末５０は、入力装置、出力装置（表示装置、スピーカを含む）を備えるのが好ましい。プロバイダ４０は、サーバ装置であるのが好ましい。処理装置が、プログラムに従って処理を実行することによって、各装置の機能が実現される。

以下、コンテンツにプロバイダＩＤを透かしで挿入する場合について説明する。

【００１４】

コンテンツ・ホルダ２０が所有するコンテンツ１０１がプロバイダ４０から端末５０に配信されて利用される場合を例に説明する。

【００１５】

まず、コンテンツ１０１をコンテンツ・ホルダ２０からコンテンツ保証機関３０に送る。コンテンツ保証機関３０は、プロバイダ４０のプロバイダＩＤを透かし挿入機能３１を用いて埋め込む。プロバイダＩＤとは、プロバイダを一意に識別するための識別子である。ここで、プロバイダ４０のプロバイダＩＤをＰ１と

する。透かしの改ざんを防ぐために、一度書きこまれた透かしは書き換え不可能な仕組みを設けるようにする。コンテンツ１０１はプロバイダＩＤを埋め込まれてコンテンツ１０２となる。コンテンツ保証機関３０が、コンテンツ１０２をプロバイダ４０に送信し、プロバイダ４０が、コンテンツ１０２をコンテンツＤＢ４５に登録する。プロバイダ４０にコンテンツを渡す前に書き換えできないプロバイダＩＤを埋め込むことにより、プロバイダ４０がプロバイダＩＤを改ざんして配信する不正を防ぐことができる。コンテンツ保証機関３０がコンテンツの仲介を行うのではなく、透かしの埋め込みだけを行い、コンテンツ・ホルダ２０からプロバイダに直接コンテンツを流しても構わない。透かしの埋め込みについては、特開2001-256192号公報等に記載されている。

【００１６】

プロバイダ４０はプロバイダ証明書４１を所有する。プロバイダ証明書４１は認証局１０が発行する証明書であり、この証明書を所有するプロバイダは本実施例の方式でコンテンツを配信できるプロバイダである。ただし、プロバイダが不正なコンテンツを流すなどした場合には証明書は無効となる。無効な証明書のリストがＣＲＬ（Certificate Revocation List）４４である。認証局１０がＣＲＬ４４を作成して、コンテンツ保証機関３０へ配布し、さらに、コンテンツ保証機関３０がＣＲＬ４４をプロバイダ４０へ配布する。また、認証局１０がＣＲＬ４４を端末５０へ配布する。また、証明書に有効期限（例えば、１週間、１か月等）を設け、頻繁に新規の証明書を発行するようにし、期限の切れた証明書は無効とみなすことによって、ＣＲＬを用いずにプロバイダ証明書の有効性を保持する方法も考えられる。

【００１７】

端末５０は、利用者からコンテンツ受信要求を受け、その要求の応答して、プロバイダ４０にコンテンツ１０２の配信を要求する場合、まず、端末５０はプロバイダチェック機能６２を使ってプロバイダの正当性をチェックする。

【００１８】

図２は、プロバイダチェック機能６２の処理の流れを示した図である。プロバイダ認証機能５１は、プロバイダ証明書４１を参照してプロバイダ認証を行う。

端末５０は、コンテンツの配信要求に先立って、プロバイダ証明書４１を、プロバイダ４０に要求する。端末５０は、そのプロバイダ証明書４１の要求に対して、プロバイダ証明書４１をプロバイダ４０から受信した場合に、プロバイダ４０がプロバイダ証明書を所有しており、プロバイダ認証が成功すると判定し、一方、プロバイダ証明書４１をプロバイダ４０から受信できない場合に、プロバイダ４０がプロバイダ証明書４１を所有しておらず、プロバイダ認証が失敗したと判定する（２１１）。プロバイダ認証が失敗した場合は無認可プロバイダであると判断し（２１２）、プロバイダ認証を終了する（２４１）。プロバイダ認証が成功した場合は、ＣＲＬ４４にプロバイダ証明書４１の証明書番号が記載されていないかを確認し（２２１）、書かれていなければ認可プロバイダであると判断する（２２２）。ＣＲＬ４４にプロバイダ証明書４１の証明書番号が記載されている場合は無認可プロバイダであると判断し（２３１）、プロバイダチェックの処理を終了する（２４１）。

【００１９】

一方、プロバイダ４０は端末５０が本方式によるコンテンツ保護機能に対応しているか否かを端末認証機能４２を用いて判断し、対応している場合には配信機能４３を用いてコンテンツ１０２を端末５０へ配信する。一方、対応していない場合には配信を中断又は中止する。端末５０が本方式によるコンテンツ保護機能に対応しているか否かは端末が固有に所有する端末ＩＤ５２をチェックするなどして判断する。つまり、プロバイダ４０が、本方式によるコンテンツ保護機能に対応している端末ＩＤを記憶しておき、コンテンツを配信する際に、端末５０から受信した端末ＩＤ５２と予めプロバイダ４０に記憶する端末ＩＤを比較し、両者の端末ＩＤが一致した場合に、対応端末と判断し、両者ＩＤが一致しない場合に、対応端末でないと判断する。対応端末にのみコンテンツを配信することにより、コンテンツの流通経路をチェックする機能を持たない端末へのコンテンツ配信を防ぐことができる。ただし、端末認証機能４２は必須機能ではない。端末認証機能４２がない場合は本方式のコンテンツ保護機能に対応していない端末にコンテンツが配信されて利用されるであろうし、そのコンテンツが他の端末にコピーされて利用される可能性も高い。コンテンツが端末間でコピーされたとしても

、大量にコピーされなければ被害は少ないが、悪質なプロバイダによって大量に配信されたり、利用者間で大量にコピーされたりして被害が拡大するおそれもある。このような場合であっても、本方式のライセンスチェック機能を設けた端末が市場に出回っていれば、その端末で不正コンテンツを検出できるため、被害が広がる前に不正に出回っているコンテンツをたやすく見つけることができる。従って、端末認証機能４２は必須機能ではないが、端末認証機能４２を設けることによってコンテンツの流出防止レベルを高くすることができる。

【００２０】

図３は端末５０におけるコンテンツ受信の流れを示している。プロバイダチェック機能６２でプロバイダが認可されているか否かを判断した後、認可プロバイダである場合には（３１１）、受信機能５３を用いてコンテンツを受信する（５３）。受信されたコンテンツに名前を付けてコンテンツ記憶部５４に保存する（３２１）。また、プロバイダ証明書４１からプロバイダＩＤpl1を読み出し、コンテンツ名と組にしてライセンス管理部５５に記憶する（３３１）。ライセンス管理部５５は、コンテンツ蓄積部（例えば、ハードディスクやフラッシュメモリ等）に比較して、耐タンパ性が高い領域（耐タンパ構造を持つ領域、例えば、ＩＣカードチップ等）である。プロバイダＩＤは、プロバイダ証明書に記載されている。ここではプロバイダ４０のプロバイダ証明書４１には、プロバイダＩＤとしてｐ１が記載されているものとし、コンテンツ名ｎ１と配信元プロバイダＩＤｐ１を５６としてライセンス管理部５５に記憶する。

【００２１】

無認可プロバイダの場合は受信機能５３を用いてコンテンツを受信する（５３）。コンテンツに名前を付けてコンテンツ記憶部５４に保存する（３２１）、コンテンツ受信の処理を終了する（３４１）。ライセンス管理部５５にコンテンツ名と配信元プロバイダＩＤの組５６を記憶するのは、以下の理由による。コンテンツに埋めこまれたプロバイダＩＤはコンテンツを配信するはずのプロバイダの識別子であり、実際の配信元プロバイダの識別子はプロバイダ証明書に記載されたプロバイダＩＤである。プロバイダＩＤは認証局が管理し発行しているため、正規の流通経路で配信されたコンテンツであれば両者は同じＩＤとなる。従って

、コンテンツに埋めこまれたプロバイダＩＤと配信元プロバイダＩＤを比較することにより、コンテンツの流通経路の正当性を判断することが可能となる。この判断がいつでもできるようにするために、コンテンツ名と配信元プロバイダＩＤの組５６をライセンス管理部５５に記憶する。この情報５６はコンテンツの流通経路の正当性を保証するための一種のライセンスと考えることができ、ライセンスを端末側で自動的に生成することが可能となる。ライセンス管理部５５は不正アクセスや改ざんを防止するための耐タンパ構造となっているため、コンテンツ名と配信元プロバイダＩＤの組５６をユーザが改ざんすることはできない。耐タンパ構造とは、外部からの不正なアクセスに備えるための物理的・論理的技術を組み込んだ構造をさし、既にＩＣカードなどの分野で実用になっている。尚、一般的に、下流側装置（クライアント装置）がコンテンツを受信する場合に、下流側装置から上流側装置（サーバ装置）へ下流側装置の証明書を送信し、上流側装置がその証明書を用いて下流側装置を認証する。しかし、本発明では、下流側装置がコンテンツを受信する場合に、上流側装置から下流側装置へ上流側装置の証明書を送信し、下流側装置がその証明書を用いて上流側装置を認証することに特徴がある。

【００２２】

ここまでコンテンツ・ホルダ２０、コンテンツ保証機関３０、プロバイダ４０を別々の機関として説明したが、全部、あるいは、一部を一つの機関が兼ねてもよい。

【００２３】

次に、端末でのコンテンツ利用時の流れを説明する。まず、ライセンスチェック機能５９によってコンテンツの流通経路の正当性を判断し、次に、流通経路が不正でなければコンテンツ利用機能６０によって音楽の再生や映像の再生などを行ない、流通経路が不正であれば不正通知機能６１によって認証局１０その他の機関へ通知する。

【００２４】

図４はプロバイダＩＤを使用したライセンスチェック４００の流れを示した図である。ライセンスチェックにはプロバイダＩＤ以外にコンテンツＩＤやユーザ

ＩＤを使用する方法も考えられるため、図１ではそれらを総称してライセンスチェック機能５９と表している。プロバイダＩＤを使用したライセンスチェック４００では、まず、透かし検出機能５８によってコンテンツに埋めこまれた透かしの検出を行い、次に、プロバイダＩＤが検出されたか否かを判断する（４１１）。プロバイダＩＤが検出されない場合は「コンテンツの流通経路は管理対象外」であると判断して処理を終了する（４８１）。

【００２５】

プロバイダＩＤが検出された場合は、透かしで検出されたプロバイダＩＤをＰ１の値とし、再生するコンテンツのコンテンツ名をコンテンツ蓄積部５４から読み出し（４３１）、該当するコンテンツ名がライセンス管理部５５に記憶されているか否かを判断する（４４１）。コンテンツ名が記憶されていない場合はライセンス管理部５５にライセンス情報５６が存在しないため、コンテンツが端末間で不正にコピーされたか、あるいは不正プロバイダが正規のプロバイダのコンテンツを流通させたかの可能性が考えられるため「コンテンツの流通経路は不正」であると判断して処理を終了する（４８１）。

【００２６】

処理４４１においてコンテンツ名が記憶されていると判断された場合は、ライセンス情報５６の配信元プロバイダＩＤの値をｐ１とし、Ｐ１とｐ１の値を比較する（４６１）。Ｐ１とｐ１の値が等しい場合は「コンテンツの流通経路は正規である」と判断し（４７１）、Ｐ１とｐ１の値が不等な場合は正規の流通経路ではないため「コンテンツの流通経路は不正である」とあると判断して（４６２）処理を終了する（４８１）。透かし検出機能５８及びライセンスチェック機能５９は、コンテンツの利用時に動作してもよいし、プロバイダ４０からコンテンツの受信及びコンテンツ蓄積部１０３への記録時に動作してもよい。

【００２７】

図７を用いて、プロバイダＩＤを使用したコンテンツ利用の流れを説明する。図７にはユーザＩＤとプロバイダＩＤとコンテンツＩＤを使用したコンテンツ利用の流れを示しているが、ここではプロバイダＩＤのみを使用するので、ユーザＩＤを使用したライセンスチェック６００、および、コンテンツＩＤの検出５０

０に関連する処理は行なわない。まず、利用者からコンテンツ利用要求と受け、その要求に応答して、プロバイダＩＤを使用したライセンスチェック４００を行ない、その結果が「コンテンツの流通経路は正規」であった場合（７１１）はステップ６００、７２１、７２２、６１の処理は省略し、コンテンツ利用機能６０によってコンテンツを利用する。「コンテンツの流通経路は不正」であった場合（７２１）はエラーである旨を表示し（７２２）、不正通知機能６１によって認証局１０に通知し、コンテンツの利用は中止して処理を終了する（７４１）。「コンテンツの流通経路は管理外」であった場合（７３１）はステップ５００、７３２、７２２、６１、および、６００、７２１、７２２の処理を省略してコンテンツ利用機能６０によってコンテンツを利用して処理を終了する（７４１）。

図８は、プロバイダＩＤを使用したコンテンツの流通経路管理と端末での利用の可否を示した図がである。端末にて不正を検出したときにはコンテンツの利用を中止するだけでもよく、不正通知機能６１はなくてもよし、コンテンツ蓄積部５４からコンテンツを削除してもよい。また、端末５０は、コンテンツ・ホルダ２０やコンテンツ保証機関３０へ不正通知を行ってもよい。

【００２８】

コンテンツを配信するプロバイダのＩＤを透かしでコンテンツに埋めこみ、一度埋めこまれた透かしは書き換えできないようにすることによって、コンテンツの配信者を特定するための情報をコンテンツと共に流通させることが可能となる。コンテンツの利用時にはコンテンツを実際に配信したプロバイダのＩＤと透かしに埋めこまれたプロバイダＩＤとを比較し、不正な流通経路の場合はコンテンツの利用を中止する機能を設けることによって、コンテンツの不正な利用を防止することが可能となる。さらに、不正な流通が端末で検出された場合にコンテンツ保証機関に不正を通知する機能を設けることにより、不正を取り締まるためのネットポリスを設けることなく、端末で不正が検出できるようになる。また、不正通知機能を設けなくても不正なプロバイダから配信されたコンテンツは端末で利用できないため、不正プロバイダの信用がなくなることが予想され、十分な不正抑止効果が期待できる。

【００２９】

近年ではコンテンツにメタデータと呼ばれるコンテンツの属性をコンテンツのヘッダ部などに付随している場合が多く、メタデータとしてコンテンツＩＤが付随している場合もある。図１ではライセンス管理部５５にコンテンツ名と配信元プロバイダの組で構成されるライセンス情報５６を記憶するようにしたが、メタデータにコンテンツＩＤが付随している場合は、コンテンツ名と配信元プロバイダＩＤの組の代わりにコンテンツＩＤと配信元プロバイダＩＤの組をライセンス情報６０２としてライセンス記憶部５５に記憶してもよい。ライセンス情報５６にコンテンツＩＤを使用する場合は図４のステップ４３１および４４１においてコンテンツ名の代わりにコンテンツＩＤを使用する。また、メモリカードなどのポータブルなメディアにライセンス管理部５５とコンテンツ蓄積部５４を設けコンテンツを移動させて利用できるようにすることも考えられる。

【００３０】

コンテンツ１０３、および、ライセンス５６はファイルの形で存在する必要はない。例えば、ストリーミング技術によりコンテンツを受信しながら利用する場合はコンテンツの一部が端末の主記憶領域に存在する。従って、コンテンツ蓄積部５４とライセンス管理部５５は主記憶であっても構わない。ストリーミング技術に本方式を適用する場合は、コンテンツの利用と同時にプロバイダＩＤの透かし検出を行い、コンテンツ利用が不可と判断した時点でコンテンツの利用を中止するなどの処理を行う。

【００３１】

次に、コンテンツにコンテンツＩＤとプロバイダＩＤを透かしで挿入する場合について説明する。

【００３２】

プロバイダＩＤに加えてコンテンツＩＤを透かしで挿入する方法も考えられる。例えば、コンテンツ・ホルダ２０が透かし挿入機能３１によってコンテンツ１０１にコンテンツＩＤを挿入する。コンテンツＩＤは認証局が管理し、例えばＩＤの上位にはコンテンツ・ホルダごとに決められたＩＤを使用するなどして、どのコンテンツ・ホルダが所有するコンテンツかが分かるようなＩＤを付与する。認証局はコンテンツ・ホルダのＩＤのみを管理し、コンテンツ・ホルダ内でコン

テンツＩＤを付与しても良い。コンテンツＩＤの透かし挿入は、各コンテンツ・ホルダからコンテンツ保証機関３０に依頼しても良いが、コンテンツＩＤにはそのコンテンツを所有するコンテンツ・ホルダを一意に識別するための識別子が組み込まれているため、プロバイダにコンテンツを渡す前にきちんとコンテンツ・ホルダがコンテンツＩＤを確認できることが不正な流通を防ぐためには必要であり、プロバイダにおいてコンテンツＩＤを挿入するのは危険である。

【００３３】

図５にコンテンツＩＤの検出の流れ５００を示す。透かし検出機能５８によってコンテンツの透かしを検出し、コンテンツＩＤが検出された場合（５２１）は、「コンテンツＩＤあり」と判断し（５２２）、そうでなければ「コンテンツＩＤなし」と判断して（５３１）終了する（５４１）。

【００３４】

図７を用いて、コンテンツＩＤとプロバイダＩＤを用いた場合のコンテンツ利用の流れを説明する。ここではユーザＩＤは使用しないので、ユーザＩＤに関する処理は省略する。プロバイダＩＤを使用した場合のコンテンツ利用の流れと同様にプロバイダＩＤを使用したライセンスチェック４００の後、ステップ４００の処理結果によって異なる処理を行なう。ステップ７１１、ステップ７２１の後はプロバイダＩＤを使用した場合のコンテンツ利用の流れと同じ処理を行なう。ステップ７３１においてコンテンツの流通経路が管理外であると判断された場合には、コンテンツＩＤの検出５００を行ない、コンテンツＩＤがあると判断された場合は（７３２）エラー表示を行ない（７２２）、不正通知機能６１を用いてコンテンツ保証機関に不正内容を通知し、コンテンツの利用を中止して終了する（７４１）。不正通知機能６１はなくてもよい。７３２においてコンテンツＩＤがないと判断された場合はコンテンツ利用機能６０によってコンテンツを利用して終了する（７４１）。

【００３５】

図９は、コンテンツＩＤとプロバイダＩＤを使用したコンテンツの流通経路管理と端末での利用の可否を示した図である。端末にて不正を検出したときには保証機関に通知せずに、コンテンツの利用を中止するだけでもよい。コンテンツＩ

Ｄの透かしがあり、コンテンツのプロバイダ流通経路が管理対象外である場合、ここではコンテンツの利用はできないようにしているが、運用によっては利用できるようにしても構わない。また、コンテンツＩＤの透かしが検出されず、コンテンツのプロバイダ流通経路が不正であると判断された場合、ここではコンテンツの利用はできないようにしているが、運用によっては、コンテンツＩＤの透かしが検出されない場合はコンテンツが利用できるようにしても構わない。運用の仕方は複数考えられるが、コンテンツ・ホルダに近い上流側でコンテンツの流通をきつく管理する場合はコンテンツＩＤの埋めこみを必須とした前提でコンテンツ利用の可否を判断するようにし、そうでない場合にはコンテンツＩＤの透かし検出はコンテンツ利用の可否に影響しないように運用すればよい。

【００３６】

このように、コンテンツにコンテンツＩＤとプロバイダＩＤを挿入することにより、コンテンツ・ホルダープロバイダ間の流通経路の確かさを確認することが可能となる。コンテンツＩＤにコンテンツ・ホルダを識別する仕組みを入れ、コンテンツにコンテンツＩＤを挿入してＩＤを書き換えできないようにすることにより、コンテンツがどのコンテンツ・ホルダからきたのかがわかるようになり、コンテンツの出所の確かさを確認できるようになる。すべてのコンテンツへのコンテンツＩＤの透かし挿入を前提とすると、コンテンツＩＤが挿入されていてプロバイダ流通経路が管理対象外である場合は不正コンテンツであり、コンテンツはコンテンツ・ホルダにてコンテンツＩＤを挿入された後、流出していたことが分かる。また、コンテンツ保証機関３０を識別できる透かしを挿入するなどさまざまな流通過程で透かしを挿入していくことによって、どこから流出したのかを検出することも可能となる。

【００３７】

次に、コンテンツにユーザＩＤを透かしで挿入する場合について説明する。

【００３８】

コンテンツを利用する機器を指定するために、機器固有の番号を組み込んだＩＤをユーザＩＤとし、ユーザＩＤをコンテンツに透かしで埋め込む方法が考えられる。ユーザＩＤとして使用できるものに、端末固有の番号や端末でコンテンツ

を利用するために必要なソフトウェアの製品番号、ＩＣカードのカード番号、メモリカードの製造番号などがあげられる。ユーザＩＤの透かし埋め込みは、プロバイダ４０に透かし挿入機能３１を設けて、コンテンツを配信する際にプロバイダ４０が行なう方法と、端末５０に透かし挿入機能３１を設けて、コンテンツ受信後に端末５０が行なう方法の二通りが考えられる。

【００３９】

図６にユーザＩＤを使用したライセンスチェック６００の流れを示す。処理が開始すると（６０１）、透かし検出機能５８がコンテンツの透かしを検出し、その結果、ユーザＩＤが検出された場合は（６１１）、Ｕ１に検出されたユーザＩＤの値を代入し（６２１）、ｕ１に端末の製造番号を代入する（６３１）。Ｕ１とｕ１の値が等しい場合は（６４１）「コンテンツの流通経路は正規である」と判断し（４７１）、層でない場合は「コンテンツの流通経路は不正である」と判断して（４４２）処理を終了する（６５１）。ステップ６１１においてユーザＩＤが検出されなかった場合は「コンテンツの流通経路は管理対象外である」と判断する（４１２）して処理を終了する（６５１）。ここでは、ユーザＩＤには端末の製造番号を使用しているが、端末を一意に識別することができさえすれば、ユーザＩＤは端末の製造番号と同じでなくてもよい。

【００４０】

ユーザＩＤを用いた場合のコンテンツ利用の流れを図７を用いて説明する。ここではコンテンツＩＤとプロバイダＩＤは使用しないので、処理を開始（７０１）すると、コンテンツＩＤとプロバイダＩＤに関する処理は省略し、ステップ６００にてユーザＩＤを使用したライセンスチェックを行ない、ステップ７２１にてコンテンツの流通経路は不正であると判断された場合はエラーを表示し（７２２）、コンテンツの利用を中止して処理を終了する（７４１）。ステップ７２１の判断が失敗した場合にはコンテンツ利用機能６０によってコンテンツを利用して処理を終了する（７４１）。

【００４１】

図１０は、ユーザＩＤを使用したコンテンツの流通経路管理と端末での利用の可否を示した図である。ここでは、端末の製造番号をユーザＩＤに使用する場合

について示している。透かしのユーザＩＤと端末製造番号が異なる場合は、利用を許可された端末とは別の端末でコンテンツ利用しようとしていると判断してコンテンツの利用を中止する。コンテンツ利用の可否や保証機関へ通知するか否かなどの運用については、この図の通りである必要はない。

【００４２】

このように、利用する端末を指定するための識別子をユーザＩＤとしてコンテンツに透かしで挿入し、利用端末においてユーザＩＤを検出して特定されるか否かによってコンテンツの利用を制限する機能を設けることにより、コンテンツを利用する端末を特定することが可能となる。また、利用者の端末から不正に流出したコンテンツには端末を識別するためのユーザＩＤが透かしで埋めこまれているため、透かしを検出することによって、どの端末からコンテンツが流出したかを確認することが可能となる。

【００４３】

次に、コンテンツにプロバイダＩＤとユーザＩＤを透かしで挿入する場合を説明する。

【００４４】

ユーザＩＤに加えてプロバイダＩＤを透かしで挿入する方法も考えられる。上述したプロバイダＩＤを挿入する場合とユーザＩＤを挿入する場合との組み合わせで実現できる。プロバイダＩＤとユーザＩＤを用いた場合のコンテンツ利用の流れを図７を用いて説明する。ここではコンテンツＩＤは使用しないので、コンテンツＩＤの検出とそれに関連する処理は省略する。処理を開始（７０１）してプロバイダＩＤを使用したライセンスチェック４００を行い、ステップ７１１にて「コンテンツの流通経路は正規」と判断された場合、ユーザＩＤを使用したライセンスチェック６００を行う。その結果、「コンテンツの流通経路は不正」と判断された場合（７２１）はエラーを表示し（７２２）、コンテンツ保証機関に通知（６１）してコンテンツの利用は中止して処理を終了（７４１）する。ステップ７２１の判断が失敗した場合はコンテンツ利用機能６０によりコンテンツを利用して処理を終了（７４１）する。ステップ７２１にて「コンテンツの流通経路は不正」と判断された場合は上述のプロバイダＩＤを用いた場合のコンテンツ

利用の流れと同様にステップ７２２、６１の処理を行って終了（７４１）する。ステップ７３１にて「コンテンツの流通経路は管理外」と判断された場合は、コンテンツＩＤに関連するステップ５００、７３２、７２２、６１の一連の処理は省略し、ステップ６００に進む。ステップ６００にてユーザＩＤを使用したライセンスチェックを行い、ステップ７２１にて「コンテンツの流通経路は不正」と判断された場合はエラーを表示（７２２））して利用を中止し、そうでない場合はコンテンツ利用機能６０によってコンテンツを利用して終了（７４１）する。

【００４５】

図１１は、プロバイダＩＤとユーザＩＤを使用したコンテンツの流通経路管理と端末での利用の可否の例を示した図である。端末での利用の可否と保証機関に通知するか否かなどについてはいろいろな運用の仕方が考えられる。例えば、プロバイダの流通経路は正規であるが端末流通経路は不正である場合、図１１ではコンテンツの利用は不可であり、保証機関に通知するようにしている。このような流通経路の例として、正規に購入した個人が不正なプロバイダになり、大量に配布してしまうという可能性も考えられる。そのようなときでも、保証機関への通知機能により、正規に配信されている数と保証機関に不正が通知された数とを比較して、明らかに不正通知件数が多い場合はそのコンテンツは不正に流通している可能性が高いと判断することもできる。その他の運用方法としては、図１１では利用不可の場合については、エラーだけを表示したり、正規のプロバイダからの購入を勧める表示をしたり、ライセンス購入用のサイトを別途設けてそのサイトに接続するなどが考えられる。

【００４６】

このように、プロバイダＩＤとユーザＩＤを透かしで挿入することでプロバイダー端末間のコンテンツの正規の流通経路をコンテンツに埋めこんで流通させることができるようになり、コンテンツの実際の流通経路とコンテンツに埋めこまれた正規の流通経路を比較することにより、プロバイダの正当性と端末の正当性を確認できるようになる。

【００４７】

次に、コンテンツにコンテンツＩＤとプロバイダＩＤとユーザＩＤを透かしで

挿入する場合を説明する。

【００４８】

コンテンツＩＤ、プロバイダＩＤ、ユーザＩＤを透かしで挿入する方法も考えられる。コンテンツＩＤとプロバイダＩＤとユーザＩＤを用いた場合のコンテンツ利用の流れを図７を用いて説明する。処理の開始（７０１）からステップ７３１までは、上述のプロバイダＩＤとユーザＩＤを用いた場合と同様である。ステップ７３１にて「コンテンツの流通は管理外」と判断した場合、コンテンツＩＤの検出（５００）を行ない、コンテンツＩＤが検出された場合は（７３２）エラーを表示し（７２２）、コンテンツ保証機関に通知して（７２２）、処理を終了する（７４１）。コンテンツＩＤが検出されなければ、プロバイダＩＤとユーザＩＤを用いた場合と同様にステップ６００、７２１、７２２、６０の処理を行なって終了する（７４１）。コンテンツＩＤがすべてのコンテンツに挿入されていることを前提とするか否かによってコンテンツ利用の流れは変わる。無料のコンテンツや個人制作のコンテンツ（無料コンテンツ）にはコンテンツＩＤが挿入されないことも想定し、ここでは、コンテンツＩＤが挿入されていない場合でもコンテンツが利用できる流れになっている。また、コンテンツＩＤが挿入されているコンテンツは必ず認可されたプロバイダ経由で配信されると想定し、コンテンツＩＤが挿入されていてプロバイダ流通経路が管理対象外である場合は、不正な配信と考えてコンテンツの利用を中止する流れになっている。

【００４９】

図１２に、コンテンツＩＤ、プロバイダＩＤ、ユーザＩＤを使用したコンテンツの流通経路管理と端末での利用の可否の例を示す。コンテンツＩＤが挿入されていないコンテンツは全て利用できない設定にしたり、各ＩＤを使ったライセンスチェックの結果が管理対象外の場合は、コンテンツの利用の流れは正規の流通経路の場合と同じとするなど、いろいろな運用が考えられる。

【００５０】

このように、コンテンツＩＤとプロバイダＩＤとユーザＩＤを透かしで挿入することにより、コンテンツ・ホルダープロバイダー端末間のコンテンツの正規の流通経路をコンテンツに埋めこんで流通させることができるようになる。コンテ

ンツに埋めこまれた透かしを検出することによってコンテンツの正規の流通経路を確認できるようになり、コンテンツの実際の流通経路とコンテンツに埋めこまれた正規の流通経路を比較することにより、コンテンツの流通経路の確かさを確認できるようになる。コンテンツの利用に際しては、確かさのレベルを判定し、その判定結果に応じて利用を制限する機能を端末に設けることにより、例えば音楽コンテンツの再生時に、確かさが低くなるのに応じて多くの雑音を挿入するようにするなど、確かさのレベルに応じた処理ができるようになる。

【００５１】

本発明によれば、コンテンツの流通経路の正当性を判断するための情報をライセンスに代用できるので、高いレベルでのコンテンツ保護ができるようになる。

【００５２】

本発明によれば、コンテンツの流通経路の正当性に応じてコンテンツの利用を制限できるので、コンテンツ・ホルダにとっては、確かな経路でコンテンツを流通させることができるという効果がある。また、コンテンツの利用者も身元の確かなコンテンツを利用できることで安心感が得られる。

【００５３】

いつくかのＩＤを組み合わせて用いたり、端末側での利用可否の判断を変更することで、保護したいコンテンツのセキュリティレベルに応じた運用ができるという効果もある。

【００５４】

コンテンツの流通経路が不正であると判断した場合は、認証局、もしくは、コンテンツ保証機関に通報する機能によって、不正なコンテンツの流通を発見することができるので、ネットポリスがふようであるという効果もある。また、通報しないまでも、不正な流通経路のコンテンツは端末での利用ができなくなるため、不正な流通が拡大しないという効果もある。

【００５５】

【発明の効果】

本発明によれば、プロバイダＩＤによってデジタルコンテンツを管理するため、コンテンツ・ホルダとコンテンツ利用者の片方又は双方に対しデジタルコンテ

ンツの流通経路を保証するという効果を奏する。

【００５６】

本発明によれば、デジタルコンテンツを不正流通したプロバイダを特定したり、不正流通したデジタルコンテンツの利用を制限するため、デジタルコンテンツの不正流通を抑制できるという効果を奏する。

【図面の簡単な説明】

【図１】

本発明の一実施例の全体の構成を示した図である。

【図２】

プロバイダチェックの流れを示した図である。

【図３】

コンテンツ受信の流れを示した図である。

【図４】

プロバイダＩＤを使用したライセンスチェックの流れを示した図である。

【図５】

コンテンツＩＤの検出の流れを示した図である。

【図６】

ユーザＩＤを使用したライセンスチェックの流れを示した図である。

【図７】

ユーザＩＤとプロバイダＩＤとコンテンツＩＤを使用したコンテンツ利用の流れを示した図である。

【図８】

プロバイダＩＤを使用したコンテンツの流通経路管理と端末での利用可否の例を表にまとめて示した図である。

【図９】

コンテンツＩＤとプロバイダＩＤを使用したコンテンツの流通経路管理と端末での利用可否の例を表にまとめて示した図である。

【図１０】

ユーザＩＤを使用したコンテンツの流通経路管理と端末での利用可否の例を表に

まとめて示した図である。

【図１１】

ユーザＩＤとプロバイダＩＤを使用したコンテンツの流通経路管理と端末での利用可否の例を表にまとめて示した図である。

【図１２】

コンテンツＩＤとプロバイダＩＤとユーザＩＤを使用したコンテンツの流通経路管理と端末での利用可否の例を表にまとめて示した図である。

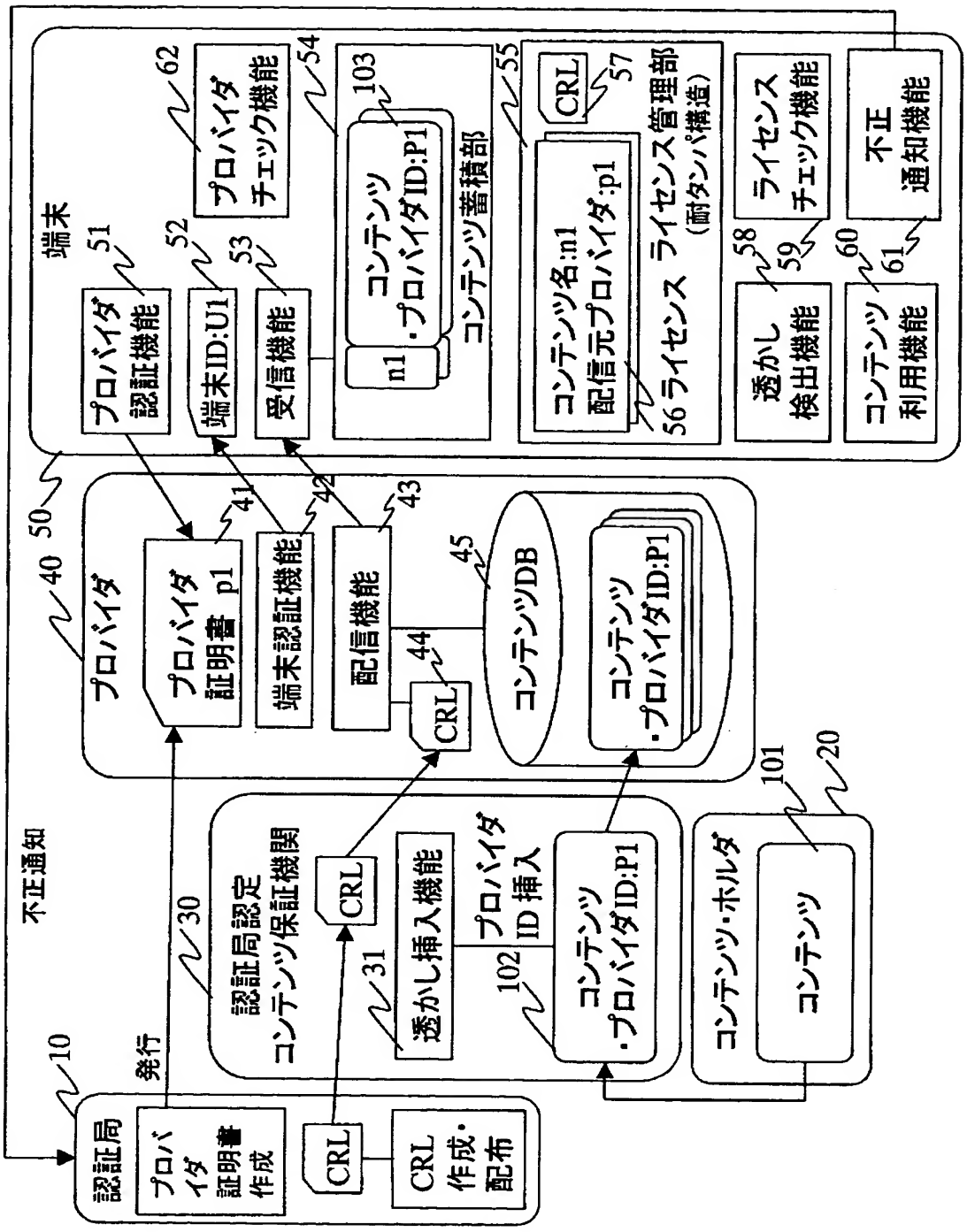
【符号の説明】

１０…認証局、２０…コンテンツ・ホルダ、３０…コンテンツ保証機関、３１…透かし挿入機能、４０…プロバイダ、４１…プロバイダ証明書、５０…端末、５１…プロバイダ認証機能、５３…受信機能、５４…コンテンツ蓄積部、５５…ライセンス管理部、５６…ライセンス、５８…透かし検出機能、５９…ライセンスチェック機能、６０…コンテンツ利用機能、６１…不正通知機能、１０１，１０２，１０３…コンテンツ。

【書類名】　図面

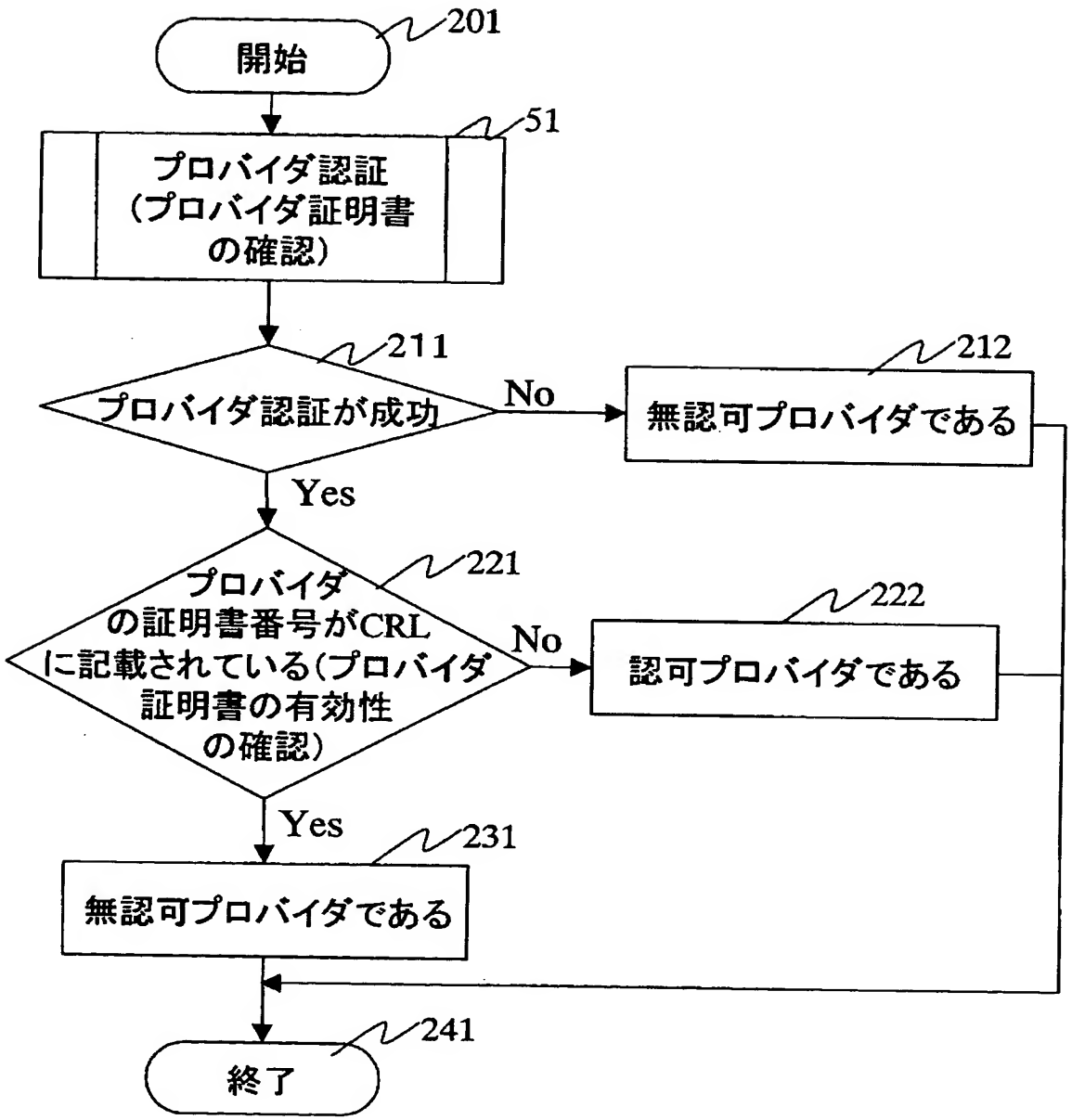
【図１】

図1


端末
プロバイダ 認証機能
端末ID:U1
受信機能
プロバイダ チェック機能
コンテンツ ・プロバイダID:P1
n1
コンテンツ蓄積部
CRL
コンテンツ名:n1 配信元プロバイダ:p1
56 ライセンス ライセンス管理部 (耐タンパ構造)
ライセンス チェック機能
不正 通知機能
透かし 検出機能
コンテンツ 利用機能
51
52
53
54
55
57
58
59
60
61
62
103
50
40
プロバイダ
プロバイダ 証明書 p1
端末認証機能
配信機能
CRL
コンテンツDB
コンテンツ ・プロバイダID:P1
41
42
43
44
45
不正通知
発行
認証局
プロバイ ダ 証明書 作成
CRL
CRL 作成・ 配布
10
認証局認定 コンテンツ保証機関
CRL
透かし挿入機能
プロバイダ ID 挿入
コンテンツ ・プロバイダID:P1
30
31
102
コンテンツ・ホルダ
コンテンツ
101
20

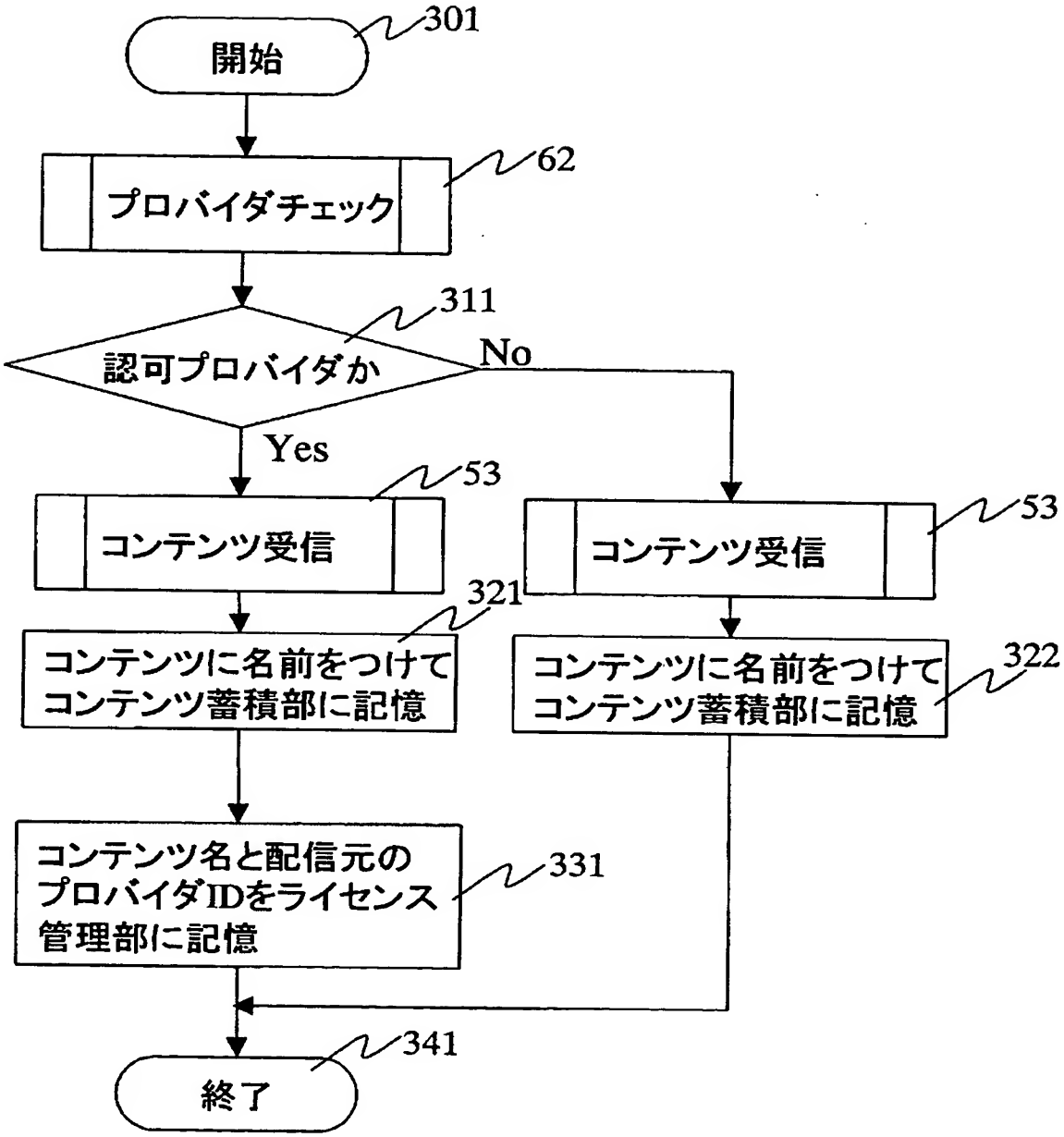
【図２】

図２


開始
201
プロバイダ認証
(プロバイダ証明書
の確認)
51
プロバイダ認証が成功
211
No
無認可プロバイダである
212
Yes
プロバイダ
の証明書番号がCRL
に記載されている(プロバイダ
証明書の有効性
の確認)
221
No
認可プロバイダである
222
Yes
無認可プロバイダである
231
終了
241

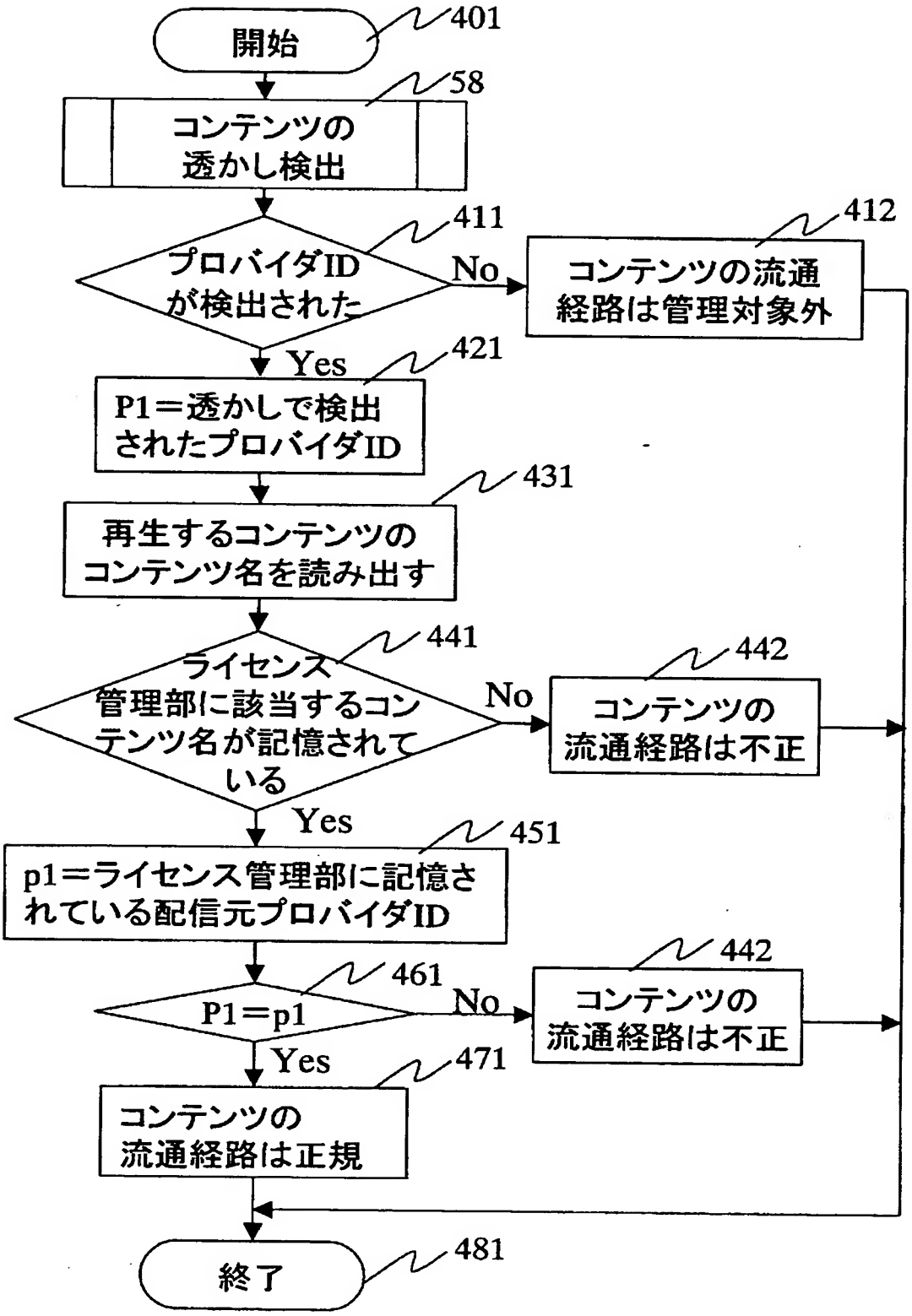
【図３】

図3


開始
301
プロバイダチェック
62
認可プロバイダか
311
No
Yes
コンテンツ受信
53
コンテンツ受信
53
コンテンツに名前をつけて
コンテンツ蓄積部に記憶
321
コンテンツに名前をつけて
コンテンツ蓄積部に記憶
322
コンテンツ名と配信元の
プロバイダIDをライセンス
管理部に記憶
331
終了
341

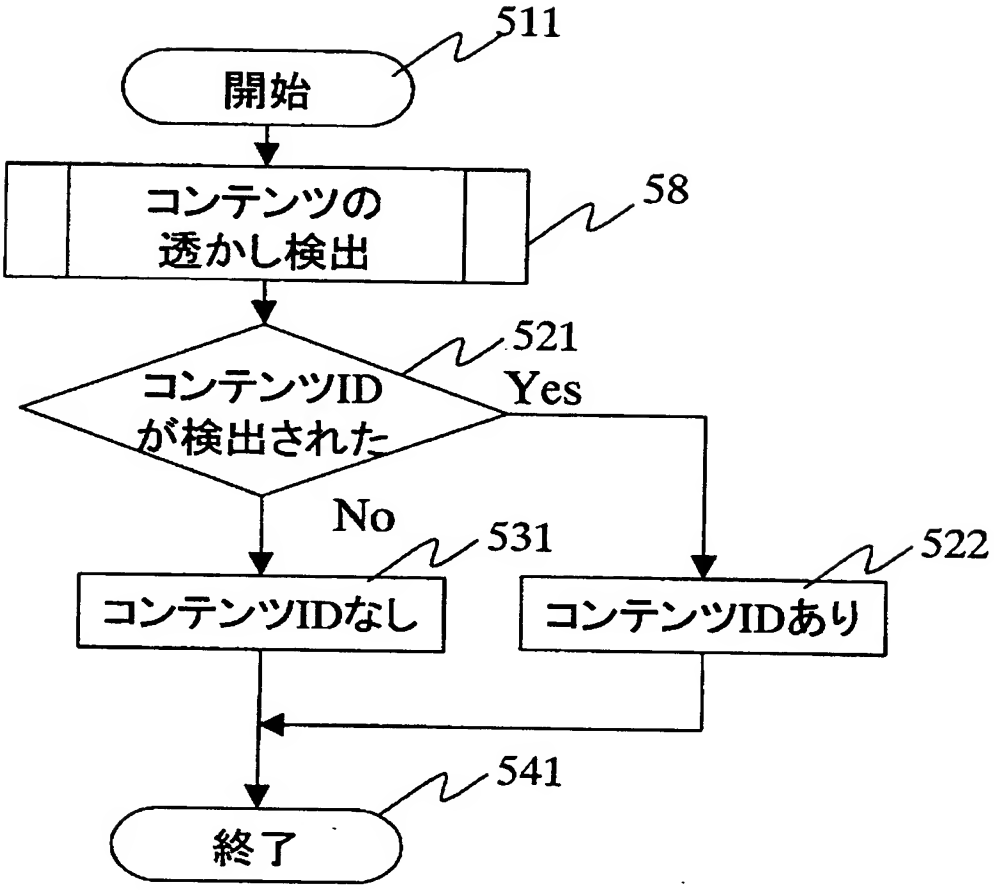
【図４】

図4


開始
401
58
コンテンツの
透かし検出
411
プロバイダID
が検出された
No
412
コンテンツの流通
経路は管理対象外
Yes
421
P1＝透かしで検出
されたプロバイダID
431
再生するコンテンツの
コンテンツ名を読み出す
441
ライセンス
管理部に該当するコン
テンツ名が記憶されて
いる
No
442
コンテンツの
流通経路は不正
Yes
451
p1＝ライセンス管理部に記憶さ
れている配信元プロバイダID
461
P1＝p1
No
442
コンテンツの
流通経路は不正
Yes
471
コンテンツの
流通経路は正規
終了
481

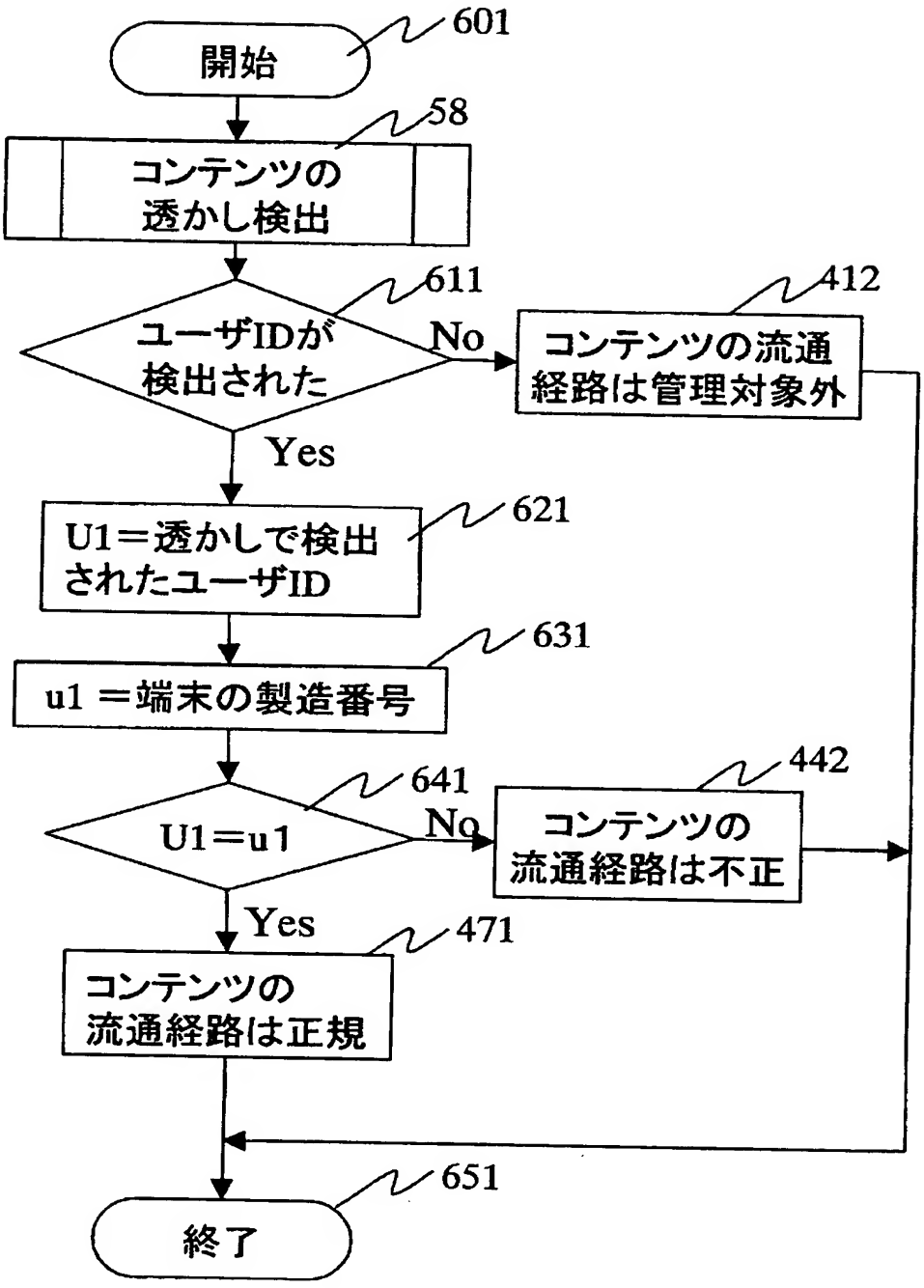
【図５】

図5


511
開始
コンテンツの
透かし検出
58
521
コンテンツID
が検出された
Yes
No
531
522
コンテンツIDなし
コンテンツIDあり
541
終了

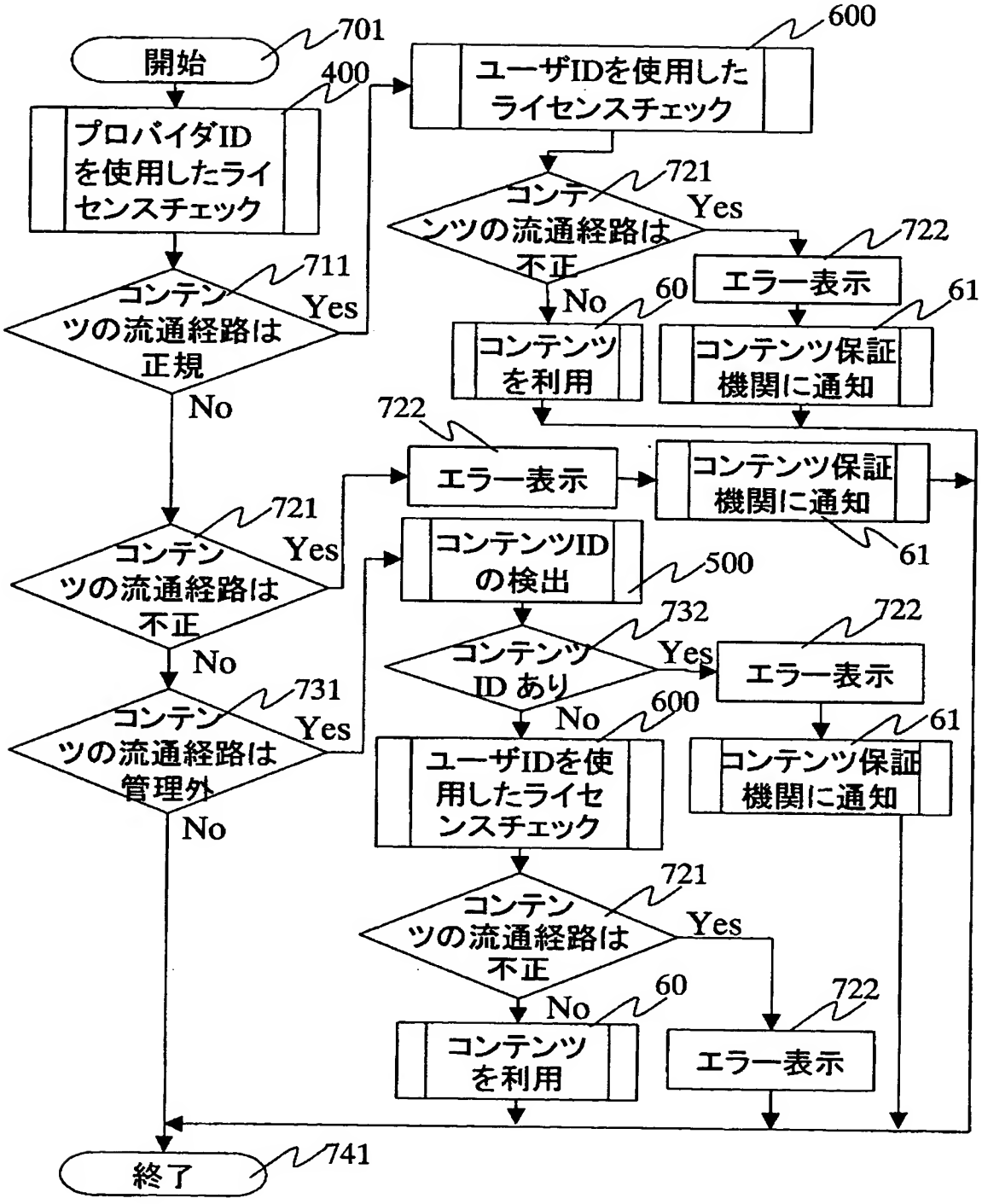
【図６】

図6


601
開始
58
コンテンツの
透かし検出
611
ユーザIDが
検出された
No
412
コンテンツの流通
経路は管理対象外
Yes
621
U1＝透かしで検出
されたユーザID
631
u1 ＝端末の製造番号
641
U1＝u1
No
442
コンテンツの
流通経路は不正
Yes
471
コンテンツの
流通経路は正規
651
終了

【図７】

図7


開始
701
プロバイダID を使用したライセンスチェック
400
コンテンツの流通経路は正規
711
Yes
No
コンテンツの流通経路は不正
721
Yes
No
ユーザIDを使用したライセンスチェック
600
エラー表示
722
コンテンツを利用
60
コンテンツ保証機関に通知
61
コンテンツIDの検出
500
コンテンツID あり
732
Yes
No
コンテンツの流通経路は管理外
731
Yes
No
終了
741

【図８】

図8

プロバイダIDの透かし ○：有 ×：無	プロバイダ認証 ○：認可 ×：無認可	透かしとプロバイダ認証によるプロバイダIDの一致 ○：一致 ×：不一致 —：比較不能	コンテンツのプロバイダ流通経路 ○：正規 ×：不正 —：管理対象外	コンテンツの利用 ○：可 ×：不可
○	○	○	○	○
		×	×	× 保証機関に通知
○	×	—	×	× 保証機関に通知
×	○	—	—	○
×	×	—	—	○

【図９】

図9

コンテンツIDの透かし ○:有 ×:無	コンテンツのプロバイダ流通経路(800(図8)) ○:正規 ×:不正 —:管理対象外	コンテンツの流通経路 ○:正規 ×:不正 —:管理対象外	コンテンツの利用 ○:可 ×:不可
○	○	○	○
×	○	○	○
○	×	×	× 保証機関に通知
×	×	×	× 保証機関に通知
○	—	×	× 保証機関に通知
×	—	—	○

【図１０】

図10

ユーザIDの透かし ○:有 ×:無	透かしのユーザIDと端末製造番号の一致 ○:一致 ×:不一致	コンテンツの端末流通経路 ○:正規 ×:不正 —:管理対象外	コンテンツの利用 ○:可 ×:不可
○	○	○	○
○	×	×	×
×	—	—	○

【図１１】

図11

コンテンツのプロバイダ流通経路(800(図8)) ○:正規 ×:不正 —:管理対象外	コンテンツの端末流通経路(900(図9)) ○:正規 ×:不正 —:管理対象外	コンテンツの流通経路 ○:正規 ×:不正 —:管理対象外	コンテンツの利用 ○:可 ×:不可
○	○	○	○
○	×	×	× 保証機関に通知
○	—	プロバイダ:○ 利用端末:—	○
×	○	×	× 保証機関に通知
×	×	×	× 保証機関に通知
×	—	×	× 保証機関に通知
—	○	プロバイダ:— 利用端末:○	○
—	×	プロバイダ:— 利用端末:×	×
—	—	—	○

【図１２】

図12

コンテンツIDの透かし ○:有 ×:無	コンテンツのプロバイダ流通経路(900(図9)) ○:正規 ×:不正 —:管理対象外	コンテンツの端末流通経路(1000(図10)) ○:正規 ×:不正 —:管理対象外	コンテンツの流通経路 ○:正規 ×:不正 —:管理対象外	コンテンツの利用 ○:可 ×:不可
○	○	○	○	○
○	○	×	×	× 保証機関に通知
○	○	—	プロバイダ:○ 利用端末:—	○
×	○	○	○	○
×	○	×	×	× 保証機関に通知
×	○	—	プロバイダ:○ 利用端末:—	○
○	×	○	×	× 保証機関に通知
○	×	×	×	× 保証機関に通知
○	×	—	×	× 保証機関に通知
×	×	○	×	× 保証機関に通知
×	×	×	×	× 保証機関に通知
×	×	—	×	× 保証機関に通知
○	—	○	×	× 保証機関に通知
○	—	×	×	× 保証機関に通知
○	—	—	×	× 保証機関に通知
×	—	○	プロバイダ:— 利用端末:○	○
×	—	×	×	×
×	—	—	—	○

【書類名】　要約書

【要約】

【課題】

本発明は、コンテンツ・ホルダとコンテンツ利用者の片方又は双方に対しデジタルコンテンツの流通経路を保証し、又は、デジタルコンテンツの不正流通を抑制することを課題とする。

【解決手段】

プロバイダ４０が配信するプロバイダ４０のプロバイダＩＤを電子透かしを用いて埋め込む。端末５０は、プロバイダ４０の証明書４１を確認し、証明書４１に記載されているプロバイダＩＤとコンテンツＩＤの組５６をライセンス管理部５５に記憶する。端末５０では、コンテンツの利用時にはプロバイダＩＤの透かしを検出し、耐タンパ領域に記憶されたプロバイダＩＤと透かしに埋め込まれたプロバイダＩＤとが一致しているかどうかによって、コンテンツの利用の可否を決定する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００２－３２１９６２
受付番号	５０２０１６７２０７６
書類名	特許願
担当官	第七担当上席　００９６
作成日	平成１４年１１月　７日

＜認定情報・付加情報＞

【提出日】　平成14年11月 6日

次頁無

出 願 人 履 歴 情 報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所